

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION  
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété  
Intellectuelle  
Bureau international



(43) Date de la publication internationale  
10 mars 2005 (10.03.2005)

PCT

(10) Numéro de publication internationale  
**WO 2005/022820 A1**

(51) Classification internationale des brevets<sup>7</sup> : H04L 9/30

(21) Numéro de la demande internationale :

PCT/EP2004/051411

(22) Date de dépôt international : 8 juillet 2004 (08.07.2004)

(25) Langue de dépôt :

français

(26) Langue de publication :

français

(30) Données relatives à la priorité :

03/09457

31 juillet 2003 (31.07.2003) FR

(71) Déposant (pour tous les États désignés sauf US) : GEM-  
PLUS [FR/FR]; Avenue du Pic de Bertagne, Parc d'activité  
de Gémenos, F-13420 GEMENOS (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants (pour US seulement) : VIL-  
LEGAS, Karine [FR/FR]; 21 rue Massilié, F-13420  
GEMENOS (FR). JOYE, Marc [BE/FR]; Traverse des  
Jardins, F-83640 SAINT ZACHARIE (FR). CHEVAL-  
LIER-MAMES, Benoit [FR/FR]; La SardannellLes  
Brayes, F-13260 CASSIS (FR).

(81) États désignés (sauf indication contraire, pour tout titre de  
protection nationale disponible) : AE, AG, AL, AM, AT,  
AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO,  
CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB,  
GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG,  
KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG,  
MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH,  
PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN,  
TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés (sauf indication contraire, pour tout titre  
de protection régionale disponible) : ARIPO (BW, GH,  
GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,  
ZW), eurasién (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),  
européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,  
FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI,  
SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,  
GW, ML, MR, NE, SN, TD, TG).

Publiée :

— avec rapport de recherche internationale

En ce qui concerne les codes à deux lettres et autres abrégia-  
tions, se référer aux "Notes explicatives relatives aux codes et  
abréviations" figurant au début de chaque numéro ordinaire de  
la Gazette du PCT.

(54) Title: METHOD FOR THE SECURE APPLICATION OF A CRYPTOGRAPHIC ALGORITHM OF THE RSA TYPE AND  
CORRESPONDING COMPONENT

(54) Titre : PROCEDE POUR LA MISE EN ŒUVRE SECURISEE D'UN ALGORITHME DE CRYPTOGRAPHIE DE TYPE  
RSA ET COMPOSANT CORRESPONDANT

(57) Abstract: The invention relates to a method for the secure application of a cryptographic algorithm of the RSA type in an  
electronic component. The method permits obtaining the value of a public exponent e from a given set of probable values, without  
a priori knowledge of said value and, having determined said value for the public exponent e, permits the application of counter-  
measures using the value of e, to block error attacks and side channel attacks, particularly of the DPA and SPA type, which may be  
carried out on the application of a private operation of the cryptographic algorithm.

(57) Abrégé : La présente invention se rapporte à un procédé pour la mise en oeuvre sécurisée d'un algorithme de cryptographie de  
type RSA dans un composant électronique. Le procédé de l'invention permet de retrouver la valeur d'un exposant public e parmi un  
ensemble de valeurs probables prédéterminées, lorsque l'on ne connaît pas cette valeur de e a priori et, une fois la valeur de l'exposant  
public e déterminée, permet la mise en oeuvre d'opérations de contre-mesure utilisant la valeur de e, visant à parer d'une part, les  
attaques dites attaques par faute et, d'autre part, les attaques dites à canaux cachés, notamment de type DPA et SPA, susceptibles  
d'être conduites lors de la mise en oeuvre d'une opération privée de l'algorithme de cryptographie.

WO 2005/022820 A1